UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,857	03/30/2007	Rached Ksontini	90500D-000083/US	4881

30593 7590 02/23/2009
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/577,857	**Applicant(s)** KSONTINI ET AL.	
	Examiner MICHAEL R. VAUGHAN	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 December 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/577,857 is presented for examination by the examiner. Claims 1-19 are pending. Claims 1, 4-5, 7-8, 11-13, and 17 are amended.

Response to Amendment

Specification

The newly submitted abstract is accepted.

Claim Objections

Claim objections have been withdrawn due to amendments.

Double Patenting

Examiner acknowledges Applicant's response to the double patenting rejection. Examiner will maintain that rejection as cited in the Office Action filed 9/8/08 until either the claims are amended enough to differentiate the conflicting claims or a terminal disclaimer is filed.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 4, 18, and 19 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 1, the amendment as filed creates a new source of indefiniteness. In the first limitation, Examiner cannot ascertain the meaning of “the identifier of an identifier of the security module". The phrase is confusing and seemingly redundant. To makes the claim even more hard to understand, an identifier is already defined in the claim.

Regarding claims 4, 18, and 19, the phrase "card type" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by "or the like" synonymous with “type”), thereby rendering the scope of the claim(s) unascertainable. See MPEP § 2173.05(d).

Appropriate correction is required.

Response to Arguments

Applicant's arguments filed 12/8/08 have been fully considered but they are not persuasive. Examiner has carefully reviewed the amended claims, the arguments, and the cited prior art but respectfully maintains that the said prior art teaches or suggests all of the limitations of the claims.

Specifically, in regards to claim 1, Minemura suggests that a cryptogram comprises a digest of the application, the identification data, and instructions intended for the security module. Upon further consideration of paragraph 0191, it appears that Minemura suggests the following. The server sends a cryptogram containing the application, the digest of the application, and information instructing the module on how to perform authentication, as well as identification data in the form of keys, random numbers, etc (0192). The process is interpreted as when the client sends the application, it also sends a digest of the application. The digest serves as an indication that the application has not been offered. This digest of course is encrypted by a secret key of the server. When the security module obtains the digest and application, it creates a digest of the application and compares it to the decrypted digest. If they match, it assumes that the application has not been altered because it is very difficult to generate the same digest from two different sources. The information sent along with this application and digest tells the security module how to proceed in obtaining the digest.

In regards to claim 17, Examiner finds support for this limitation in paragraph 0191 and Figure 28. In Figure 28, element 2802 is the security module. The outlined process being performed is aforementioned. The specification (paragraph 0192) makes it clear that the security module compares the digest received with that one it computers on the application file to verify the authenticity of the application. Again, the information sent with the digest is equivalent to the instructions of the claim.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 17 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by USP Application Publication 2003/0114144 to Minemura.

As per claim 17, Minemura teaches a security module [authentication module] comprising resources intended to be accessed locally by at least one application installed in an equipment [terminal] connected to a network (see abstract),

said equipment including means for reading and transmitting data including at least an identifier of the equipment and an identifier of the security module, said module further comprising means for reception, storage, and analysis of a cryptogram (Figure 6) containing among other data, a digest of said application (0193) and instructions (0125),

means for verification of said application (0192), and

means for extraction and execution of the instructions contained in the cryptogram, for at least one of blocking certain resources according to the result of the verification of the application (0085-0089).

As per claim 18, Minemura teaches the security module [IC] is at least one being of the "subscriber module" and " SIM card" type intended to be connected to a mobile equipment (0013).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-11 and 13-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP Application Publication 2003/0114144 to Minemura.

As per claim 1 Minemura teaches an authentication method of at least one application working in a equipment [terminal] connected by a network to a control server [server/service company], said equipment being locally connected to a security module [authentication module], said application being at least one of loaded loadable and executable via an application execution environment of the equipment and being adapted to use resources stored in the security module, the method comprising (see abstract):

reception by the control server, via the network, of data comprising at least the identifier of the equipment and the identifier of the security module (0192-0193),

analysis and verification by the control server of said data (0192),

generation of a cryptogram comprising a digest of the application (0084-0085 and Fig.

6), data identifying [unique information] the equipment and the security module [identifier] and instructions intended for said module (0125),

transmission of said cryptogram, via the network and the equipment, to the security module (0085), and

verification of the application by comparing the digest extracted from the cryptogram received with a digest determined by the security module (0085),

wherein, during at least one of initialization and activation of the application, the security module executes the instructions extracted from the cryptogram and at least one of releases and blocks access to certain resources of said security module according to a result of the verification suited to this application carried out previously (0085). In one of the first of many embodiments Minemura teaches that a server downloads the application and authentication information (the hash of the application) to the terminal device (0085). In a later embodiment, Minemura teaches that the terminal and its authentication module must first authentication itself to the server before the server will initiate any data transfer (0192). Furthermore Minemura teaches that the authentication module must and is thereby authenticated with the terminal device which is authenticated by the server. So there is authentication between all three entities. Minemura explicitly teaches that the terminal device and authentication module can be identified by unique information i.e. production number, unit type number, identifier stored in ROM, and version number. Even though Minemura does not explicitly teach that the cryptogram sent for module includes this identifying data when the digest is sent, one of ordinary skill in the art would further use identifying material to thwart a malicious sender from deceiving the terminal. Minemura uses this information for authentication purposes between the authentication module and the terminal device. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to include the identifying information of the terminal [equipment] and authentication module [security module] when the digest is sent from the server to the device to prevent a man-in-the-middle attack whereby a false server sends a malicious data. Once the terminal authenticates itself by providing unique identifying information, the server can include this information in encrypted form back to the terminal to prove the server is in fact the server to which the terminal intended to communicate with.

As per claim 2, Minemura teaches the equipment is a mobile equipment of mobile telephony (0013).

As per claim 3, Minemura teaches the network is a mobile network of at least one of the type GSM or GPRS or UMTS (0013). It is notoriously well known that cell phones use these types of networks to communicate.

As per claim 4, Minemura teaches the security module is a subscriber module inserted into the mobile equipment of mobile telephony of the SIM card type (0013).

As per claim 5, Minemura teaches the identification of at least one of the set mobile equipment and subscriber module is carried out from the identifier of the mobile equipment and from the identifier of the subscriber module suited to a subscriber to the network (0193).

As per claim 6, Minemura teaches the instructions included in the cryptogram received by the security module condition the use of the applications according to criteria established previously by at least one of the operator, the application supplier, and the user of the equipment (0125, 0141).

As per claim 7, Minemura teaches the criteria define limits of use of an application according to the risks associated with at least one of the software of said application and with the hardware of the equipment that the operator desires to take into account (0125, 0141 and solves the problem of 0008).

As per claim 8, Minemura teaches the verification of the application with the cryptogram is carried out at the time of at least one of the first initialization and the first use of said application (0210).

As per claim 9, Minemura teaches the verification of the application with the cryptogram is periodically carried out at a given rate [expiry rate] according to instructions originating from the control server (0143-0144).

As per claim 10, Minemura teaches the verification of the application with the cryptogram is carried out at the time of each initialization of said application on the equipment (0144).

As per claim 11, Minemura teaches the cryptogram is generated with the aid of an asymmetrical or symmetrical encryption key from a data set (0199) containing, among other data, the identifier of the equipment, the identifier of the security module, an identifier of the application (0141), the digest of the application calculated with an unidirectional hash function and identifiers of the resources of the security module and instructions for locking/releasing of resources of the security module (0191).

As per claim 13, Minemura teaches the security module transmits to the control server, via the equipment and the network, a confirmation message when said security module has accepted or refused a cryptogram of an application (0087, provision of service).

As per claim 14, Minemura teaches the cryptogram is transmitted to the security module at the same time as the application is loaded into the equipment via the execution environment of the applications (0210).

As per claim 15, Minemura teaches the application, once loaded into the equipment from the control server via the network, requests a cryptogram from the server at the time of its initialization and transmits said cryptogram to the security module (0089), the confirmation message of acceptance or refusal of the cryptogram being transmitted by the security module to the server via the application (0210).

As per claim 16, Minemura teaches the equipment is a Pay-TV decoder or a computer to which the security module is connected (0078).

As per claim 19, Minemura teaches the security module is a subscriber module [IC] inserted into the mobile equipment of mobile telephony of the SIM card type (0013).

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Minemura in view of USP Application Publication 2002/0012433 to Haverinen et al, hereinafter Haverinen.

As per claim 12, Minemura is silent in disclosing a predictable variable in the cryptogram. Minemura does teach using a random number to prevent replay attacks

(0192). Haverinen teaches that timestamps can be used as a substitute to random number in authentication to prevent replay attacks. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the timestamps in the cryptograms as a means to prevent malicious replay attacks by a third party. Timestamps are a known to be an adequate method of performing the same function of a random number in the art of computer security.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Syed Zia/

Primary Examiner, Art Unit 2431